EXHIBIT A

C 3 2

Return Date: No return date scheduled
Hearing Date: 7/27/2020 10:30 AM - 10:30 AM
Courtroom Number: 2102
Location: District 1 Court
Cook County, IL

FILED
3/30/2020 1:15 PM
DOROTHY BROWN
CIRCUIT CLERK
COOK COUNTY, IL
2020CH03579

8982565

2120 - Served **2121 - Served**
2220 - Not Served **2221 - Not Served**
2320 - Served By Mail **2321 - Served By Mail**
2420 - Served By Publication **2421 - Served By Publication**
Summons - Alias Summons **(08/01/18) CCG 0001 A**

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS

Jeri Cotton
(Name all parties)
v.
Ring LLC

Case No. 2020-CH-03579

☑ SUMMONS ☐ ALIAS SUMMONS

To each Defendant: Ring LLC c/o Corporation Service Company, 251 Little Falls Drive, Wilmington, DE 19808

YOU ARE SUMMONED and required to file an answer to the complaint in this case, a copy of which is hereto attached, or otherwise file your appearance and pay the required fee **within thirty (30) days after service of this Summons,** not counting the day of service. To file your answer or appearance you need access to the internet. Please visit www.cookcountyclerkofcourt.org to initiate this process. Kiosks with internet access are available at all Clerk's Office locations. Please refer to the last page of this document for location information.

If you fail to do so, a judgment by default may be entered against you for the relief requested in the complaint.

To the Officer:

This Summons must be returned by the officer or other person to whom it was given for service, with endorsement of service and fees, if any, immediately after service. If service cannot be made, this Summons shall be returned so endorsed. This Summons may not be served later than thirty (30) days after its date.

Summons - Alias Summons **(08/01/18) CCG 0001 B**

E-filing is now mandatory for documents in civil cases with limited exemptions. To e-file, you must first create an account with an e-filing service provider. Visit http://efile.illinoiscourts.gov/service-providers.htm to learn more and to select a service provider. If you need additional help or have trouble e-filing, visit http://www.illinoiscourts.gov/FAQ/gethelp.asp, or talk with your local circuit clerk's office.

Atty. No.: 63746

Atty Name: Kyle Shamberg

Atty. for: Plaintiff

Address: 111 W. Washington Street #1240

City: Chicago

State: IL Zip: 60602

Telephone: (312) 750-1265

Primary Email: kshamberg@carlsonlynch.com

Witness: 3/30/2020 1:15 PM DOROTHY BROWN

DOROTHY BROWN, Clerk of Court

Date of Service: _____

(To be inserted by officer on copy left with Defendant or other person):

CLERK OF THE CIRCUIT COURT OF COOK COUNTY OFFICE LOCATIONS

Richard J Daley Center
50 W Washington
Chicago, IL 60602

District 2 - Skokie
5600 Old Orchard Rd
Skokie, IL 60077

District 3 - Rolling Meadows
2121 Euclid
Rolling Meadows, IL 60008

District 4 - Maywood
1500 Maybrook Ave
Maywood, IL 60153

District 5 - Bridgeview
10220 S 76th Ave
Bridgeview, IL 60455

District 6 - Markham
16501 S Kedzie Pkwy
Markham, IL 60428

Domestic Violence Court
555 W Harrison
Chicago, IL 60607

Juvenile Center Building
2245 W Ogden Ave, Rm 13
Chicago, IL 60602

Criminal Court Building
2650 S California Ave, Rm 526
Chicago, IL 60608

Daley Center Divisions/Departments

Civil Division
Richard J Daley Center
50 W Washington, Rm 601
Chicago, IL 60602
Hours: 8:30 am - 4:30 pm

Chancery Division
Richard J Daley Center
50 W Washington, Rm 802
Chicago, IL 60602
Hours: 8:30 am - 4:30 pm

Domestic Relations Division
Richard J Daley Center
50 W Washington, Rm 802
Chicago, IL 60602
Hours: 8:30 am - 4:30 pm

Civil Appeals
Richard J Daley Center
50 W Washington, Rm 801
Chicago, IL 60602
Hours: 8:30 am - 4:30 pm

Criminal Department
Richard J Daley Center
50 W Washington, Rm 1006
Chicago, IL 60602
Hours: 8:30 am - 4:30 pm

County Division
Richard J Daley Center
50 W Washington, Rm 1202
Chicago, IL 60602
Hours: 8:30 am - 4:30 pm

Probate Division
Richard J Daley Center
50 W Washington, Rm 1202
Chicago, IL 60602
Hours: 8:30 am - 4:30 pm

Law Division
Richard J Daley Center
50 W Washington, Rm 801
Chicago, IL 60602
Hours: 8:30 am - 4:30 pm

Traffic Division
Richard J Daley Center
50 W Washington, Lower Level
Chicago, IL 60602
Hours: 8:30 am - 4:30 pm

12-Person Jury

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
CHANCERY DIVISION

JERI COTTON, individually and on behalf of all others similarly situated,

Plaintiff,

v.

RING LLC, a Delaware limited liability company,

Serve Registered Agent:
Corporation Service Company
251 Little Falls Drive, Wilmington DE 19808

Defendant.

Case No. 2020CH03579

(JURY TRIAL DEMANDED)

CLASS ACTION COMPLAINT

Plaintiff, Jeri Cotton ("Plaintiff"), individually and on behalf of all others similarly situated, by and through her attorneys, brings this class action complaint pursuant to 735 ILCS 5/2-801, *et seq.*, against Ring LLC ("Ring"), for violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"), and alleges as follows:

NATURE OF ACTION

1. Plaintiff brings this action for damages and other legal and equitable remedies resulting from the illegal actions of Ring in collecting, storing, and using Plaintiff's and other similarly-situated individuals' biometric identifiers[1] and biometric information[2] (collectively, "biometrics"), without informed written consent, in direct violation of the BIPA.

[1] A "biometric identifier" is any personal feature that is unique to an individual, including fingerprints, iris scans, DNA, and "face geometry," among others.

[2] "Biometric information" is any information captured, converted, stored, or shared based on a person's biometric identifier used to identify an individual.

2. Ring, which was purchased by Amazon in early 2018 for more than $1 billion, develops and sells Video Doorbells, which are "smart doorbells" that allow homeowners to remotely communicate with visitors standing near the doorbell. Homeowners can see, hear, and speak to visitors from the homeowners' phone, tablet, and PC. In addition to other features, the Video Doorbell allows homeowners to automatically receive alerts and high definition, live-video footage of visitors at their home as soon as the Video Doorbell detects motion or when visitors press the Video Doorbell. Users also have the option to store and save video footage of their visitors taken by the Video Doorbell. In addition to Video Doorbells, Ring develops and sells Stick Up Cams (collectively with Video Doorbells, "Ring Cameras"), which can be placed inside or outside the home and which allow for real-time mobile notifications, live HD video, and two-way voice communication between the homeowners and visitors through the Stick Up Cams.

3. In November of 2018, Ring filed patent application material that describes an advanced system of facial recognition that police can use to match the faces of people walking by Ring Cameras with a photo database of persons who are deemed "suspicious."[3] Ring's described facial recognition technology would also allow the program to scan anyone passing a home for photos of suspicious people uploaded by a homeowner and, upon a match, the person's face could be automatically sent to law enforcement.[4] Likewise, homeowners can place photographs of other individuals on an authorized persons list.[5] Moreover, by compiling videos from separate Ring

---

[3] *See Amazon's Disturbing Plan to Add Face Surveillance to Your Front Door*, American Civil Liberties Union (2018), *available at* https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-disturbing-plan-add-face-surveillance-yo-0 (last visited Mar. 26, 2020) ("ACLU Article").

[4] *See id.*

[5] *See Amazon may want to identify burglars with facial recognition tech*, CNN (2018), *available at* https://www.cnn.com/2018/11/30/tech/amazon-patent-doorbell-facial-recognition/index.html (last visited Mar. 26, 2020) ("CNN Article").

Cameras located at different angles as visitors walk past, Ring anticipates that its facial recognition software will even be able to identify faces that are partially obscured.[6] Jacob Snow, a technology and civil liberties attorney with the American Civil Liberties Union, has referred to Ring's proposed surveillance system as "Amazon's Disturbing Plan to Add Face Surveillance to Your Front Door,"[7] and has stated that "[p]eople have the right to go about their daily lives without being watched and tracked."[8]

4. In the context of Ring's subpar security and privacy practices, it has come to light that Ring shares, with its employees, the video footage captured from all of its customers' Ring Cameras and uses that footage to bolster Ring's facial recognition technology. Sources familiar with Ring's practices have disclosed that Ring stores the video feeds from its customers' Ring Cameras in unencrypted format and allows staff around the world to have essentially unfettered access to these videos.[9] In particular, a Ukrainian research team charged with improving Ring's facial recognition tools as part of its push to turn Ring Cameras into a private surveillance grid (upon information and belief, the surveillance plan Ring proposed in its recent patent filing), has had "virtually unfettered" access to *every* Ring customer's camera videos.[10] Upon information

---

[6] *See* ACLU Article.
[7] *See id.*
[8] *See* CNN Article.
[9] *Whistleblower: Amazon Ring stores your doorbell and home video feeds unencrypted and grants broad "unfettered" access to them*, BoingBoing.net, available at https://boingboing.net/2019/01/10/surveillance-a-go-go.html (last visited March 26, 2020); *For Owners of Amazon's Ring Security Cameras, Strangers May Have Been Watching Too*, TheIntercept.com, *available at* https://theintercept.com/2019/01/10/amazon-ring-security-camera/ (last visited March 26, 2020).
[10] *Id.*

and belief, Ring has been capturing and using the facial geography of individuals appearing in these videos for years.[11]

5. In response to these allegations, Ring conceded that it viewed and annotated[12] certain videos from users who have publicly shared the video on a related Ring application and who have consented to Ring's use of the videos.[13] Regardless of whether Ring received permission from its users to utilize their biometric information to develop its facial recognition abilities, it never sought – or received – permission from visitors and other non-customer third-parties who appeared in the videos and whose biometric data was taken and used by Ring.

6. The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

7. In recognition of these concerns over the security of individuals' biometrics – particularly in the City of Chicago, which was recently selected by major national corporations as a "pilot testing site[] for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias" (740 ILCS 14/5(b)) – the Illinois Legislature enacted the BIPA, which provides, *inter alia*, that a private entity like Ring may not obtain and/or possess an individual's biometrics unless it: (1) informs that person

[11] *For Owners of Amazon's Ring Security Cameras, Strangers May Have Been Watching Too*, TheIntercept.com, *available at* https://theintercept.com/2019/01/10/amazon-ring-security-camera/ (last visited Mar. 26, 2020) ("TheIntercept Article").
[12] That is, that it drew boxes around or otherwise tagged visitors that appeared in video footage.
[13] *See* TheIntercept Article.

in writing that biometric identifiers or information will be collected or stored; (2) informs that person in writing of the specific purpose and length of term for which such biometric identifiers or biometric information is being collected, stored and used; (3) receives a written release from the person for the collection of his or her biometric identifiers or information; and (4) publishes publicly-available written retention schedules and guidelines for permanently destroying biometric identifiers and biometric information. 740 ILCS 14/15(a)-(b).

8. In direct violation of each of the foregoing provisions of § 15(a) and § 15(b) of the BIPA, Ring is actively collecting, storing, and using – without providing notice, obtaining informed written consent, or publishing data retention policies – the biometrics of millions of unwitting individuals whose faces appear in video footage captured by Ring Cameras and stored by Ring.

9. Specifically, upon information and belief, Ring has created, collected, and stored millions of "face templates" – highly detailed geometric maps of the face – from countless Illinois residents whose faces were captured by Ring Cameras. Ring creates these templates using sophisticated facial recognition technology that extracts and analyzes data from the points and contours of faces that appear in videos taken by Ring Cameras and uses them to further develop its own facial recognition software, likely in an effort to achieve the facial recognition abilities proposed in its recent patent filing. Each face template that Ring extracts is unique to a particular individual in the same way that a fingerprint or voiceprint uniquely identifies one, and only one, person.

10. Plaintiff brings this action individually and on behalf of all others similarly situated to prevent Ring from further violating the privacy rights of members of the public whose faces have appeared in footage captured by Ring Cameras in Illinois, and to recover statutory

damages for Ring's unauthorized collection, storage, and use of these individuals' biometrics in violation of the BIPA.

PARTIES

11. Plaintiff is, and has been at all relevant times, a resident and citizen of Vernon Hills, Illinois.

12. Ring is a Delaware limited liability company with its headquarters at 1523 26th Street, Santa Monica, California 90404. Accordingly, Ring is a citizen of the states of Delaware and California.

JURISDICTION AND VENUE

13. This is a class action for violations of BIPA, seeking statutory and actual damages.

14. No federal question is presented by this complaint. Plaintiff brings this Complaint solely under state law and not under federal law, and, specifically, not under the United States Constitution, nor any of its amendments, nor under 42 U.S.C. §§ 1981 or 1982, nor any other federal statute, law, rule, or regulation. Plaintiff believes and alleges that a cause of action exists under state law for the conduct complained of herein.

15. This class action is brought on behalf of all individuals whose biometric information was captured by Ring within the State of Illinois.

16. Venue is proper under 735 ILCS 5/1-108 and 2-101 of the Illinois Code of Civil Procedure, as a substantial portion of the transactions giving rise to the causes of action pleaded herein occurred in Cook County. Specifically, upon information and belief, the activities giving rise to the causes of action occurred within the city of Chicago, Illinois.

FACTUAL BACKGROUND

I. Biometric Technology Implicates Consumer Privacy Concerns

17. "Biometrics" refers to unique physical characteristics used to identify an individual. One of the most prevalent uses of biometrics is in facial recognition technology, which works by scanning a human face or an image thereof, extracting facial feature data based on specific "biometric identifiers" (*i.e.*, details about the face's geometry as determined by facial points and contours), and comparing the resulting "face template" (or "faceprint") against the face templates stored in a "face template database." If a database match is found, an individual may be identified.

18. The use of facial recognition technology in the commercial context presents numerous consumer privacy concerns. During a 2012 hearing before the United States Senate Subcommittee on Privacy, Technology, and the Law, U.S. Senator Al Franken stated that "there is nothing inherently right or wrong with [facial recognition technology, but] if we do not stop and carefully consider the way we use [it], it may also be abused in ways that could threaten basic aspects of our privacy and civil liberties."[14] Senator Franken noted, for example, that facial recognition technology could be "abused to not only identify protesters at political events and rallies, but to target them for selective jailing and prosecution."[15]

19. The Federal Trade Commission ("FTC") has raised similar concerns, and released a "Best Practices" guide for companies using facial recognition technology.[16] In the

---

[14] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012), *available at* https://www.eff.org/files/filenode/jenniferlynch_eff-senate-testimony-face_recognition.pdf (last visited Mar. 26, 2020).

[15] *Id.*

[16] *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade Commission (Oct. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/facing-

guide, the FTC underscores the importance of companies' obtaining affirmative consent from consumers before extracting and collecting their biometric identifiers and biometric information from digital photographs.

II. Illinois's Biometric Information Privacy Act

20. In 2008, Illinois enacted the BIPA due to the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276. The BIPA makes it unlawful for a company to, *inter alia*, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers[17] or biometric information, unless it first:

> (l) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

740 ILCS 14/15 (b).

21. Section 15(a) of the BIPA also provides:

> A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 ILCS 14/15(a).

---

facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf (last visited Mar. 26, 2016).

[17] BIPA's definition of "biometric identifier" expressly includes information collected about the geometry of the face (i.e., facial data obtained through facial recognition technology). *See* 740 ILCS 14/10.

22. As alleged below, Ring's practices of collecting, storing, and using individuals' biometric identifiers and information -- derived from videos taken and uploaded in Illinois without informed written consent -- violate all three prongs of § 15(b) of the BIPA. Ring's failure to provide a publicly-available written policy regarding its schedule and guidelines for the retention and permanent destruction of individuals' biometric information also violates § 15(a) of the BIPA.

III. Ring Violates Illinois's Biometric Information Privacy Act

23. Upon information and belief, for years, Ring has been storing and using the video footage captured from its users' Ring Cameras. Specifically, Ring has assigned teams to manually tag individuals appearing in this video footage so that its software can capture biometric data from the video, including the tagged individual's facial geography, and use it to bolster its own facial recognition technology. Ring does so without seeking or receiving consent of every individual appearing in this video footage.

24. Upon information and belief, unbeknownst to visitors they appear in Ring Cameras' video footage, and, in direct violation of § 15(b)(1) of the BIPA, Ring's facial recognition technology scans each and every face that has been tagged by its team members, extracts geometric data relating to the unique points and contours (*i.e.*, biometric identifiers) of each face, and then uses that data to improve Ring's facial recognition technology – all without ever informing anyone of this practice.

25. In direct violation of §§ 15(b)(2) and 15(b)(3) of the BIPA, Ring never informed Illinois residents who had their face templates collected of the specific purpose and length of time for which their biometric identifiers or information would be collected, stored, and used, nor did Ring obtain a written release from any of these individuals.

26. In direct violation of § 15(a) of the BIPA, Ring does not have written, publicly-available policies identifying their retention schedules, or guidelines for permanently destroying any of these biometric identifiers or information.

IV. Plaintiff's Experience

27. Within the past two years, Plaintiff visited several homes in Illinois at which a Ring Camera was installed and, on each occasion, has appeared in the video footage taken by the Ring Cameras. Upon information and belief, Ring has accessed and used this video footage by identifying Plaintiff as she appears in the videos and has captured her biometric data by allowing its facial recognition software to scan her facial features, including the contours of her face, and the distances between her eyes, nose, and ears.

28. The resulting biometric data Ring captured, and the process by which its facial recognition program captured the biometric data, was then used to improve the capabilities of its facial recognition software.

29. Plaintiff never consented, agreed, or gave permission – written or otherwise – to Ring for the collection or storage of her unique biometric identifiers or biometric information.

30. Further, Ring never provided Plaintiff with, nor did she ever sign a written release, allowing Ring to collect or store her unique biometric identifiers or biometric information.

31. Likewise, Ring never provided Plaintiff with an opportunity to prohibit or prevent the collection, storage, or use of her unique biometric identifiers or biometric information, nor does Ring have any guidelines in place for permanently destroying any of her biometric identifiers or information.

32. Nevertheless, when Plaintiff unknowingly appeared before the Ring Cameras, Ring took that video footage, captured her facial geography, and used it to improve its facial recognition abilities, all in direct violation of the BIPA.

CLASS ALLEGATIONS

33. **Class Definition**: Plaintiff brings this action pursuant to 735 ILCS 5/2-801, individually and on behalf of a class of similarly situated individuals, defined as follows (the "Class"):

> All Illinois residents who had their biometric identifiers, including scans of their facial geometry, collected, captured, received, or otherwise obtained by Ring from videos or other visual media captured by a Ring Camera.

The following are excluded from the Class: (1) any Judge presiding over this action and members of his or her family; (2) Ring, its subsidiaries, parents, successors, predecessors, and any entity in which Ring or its parent has a controlling interest (as well as current or former employees, officers and directors); (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Ring's counsel; (6) the legal representatives, successors, and assigns of any such excluded persons; and (7) any Illinois resident who has purchased a Ring Camera.

34. **Numerosity**: Given that the number of persons within the Class includes essentially all individuals who have passed by any home with a Ring Camera, that number is undoubtedly substantial. It is, therefore, impractical to join each member of the Class as named plaintiffs. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism

is the most economically feasible means of determining and adjudicating the merits of this litigation.

35. **Commonality and Predominance**: There are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do not vary from Class member to Class member, and which may be determined without reference to the individual circumstances of any Class member include, but are not limited to, the following:

(a) whether Ring collected or otherwise obtained Plaintiff's and the Class members' biometric identifiers or biometric information;

(b) whether Ring properly informed Plaintiff and the Class members that it collected, used, and stored their biometric identifiers or biometric information;

(c) whether Ring obtained a written release (as defined in 740 ILCS 1410) to collect, use, and store Plaintiff's and the Class members' biometric identifiers or biometric information;

(d) whether Ring developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of their last interaction, whichever occurs first;

(e) whether Ring used Plaintiff's and the Class members' biometric identifiers or biometric information to identify them; and

(f) whether Ring's violations of the BIPA were committed intentionally, recklessly, or negligently.

36. **Adequate Representation**: Plaintiff has retained and is represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation. Plaintiff and her counsel are committed to vigorously prosecuting this class action. Neither Plaintiff nor her counsel have any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiff is able to fairly and adequately represent and protect the interests of the Class. Plaintiff has raised viable statutory claims of the type reasonably expected to be

raised by members of the Class and will vigorously pursue those claims. If necessary, Plaintiff may seek leave of this Court to amend this Complaint to include additional Class representatives to represent the Class, or additional claims as may be appropriate.

37. **Superiority**: A class action is superior to all other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all Class members is impracticable. Even if every member of the Class could afford to pursue individual litigation, the court system could not, and it would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent, or contradictory judgments, and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system, and protects the rights of each member of the Class. Plaintiff anticipates no difficulty in the management of this action as a class action. Class-wide relief is essential to compel compliance with the BIPA.

FIRST CAUSE OF ACTION
Violation of 740 ILCS 14/1, *et seq.*
(On Behalf of Plaintiff and the Class)

38. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

39. The BIPA makes it unlawful for any private entity to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first: "(1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier

or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information. . . ." 740 ILCS 14/15(b).

40. Ring is a Delaware limited liability company and thus qualifies as a "private entity" under the BIPA. *See* 740 ILCS 14/10.

41. Plaintiff and Class members are individuals who had their "biometric identifiers" and "biometric information," including scans of their facial geometry, collected, captured, received, or otherwise obtained by Ring from videos that were taken Ring Cameras from within the state of Illinois. *See* 740 ILCS 14/10.

42. Ring systematically and automatically collected, used, and stored Plaintiff's and Class members' biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

43. In fact, Ring failed to properly inform Plaintiff or the Class in writing that their biometric identifiers and/or biometric information was being "collected or stored" by Ring, nor did Ring inform Plaintiff or Class members in writing of the specific purpose and length of term for which their biometric identifiers and/or biometric information was being "collected, stored and used," as required by 740 ILCS 14/15(b)(1)-(2).

44. In addition, Ring does not publicly provide a retention schedule or guidelines for permanently destroying the biometric identifiers and/or biometric information of Plaintiff or Class members, as required by the BIPA. *See* 740 ILCS 14/15(a).

45. By collecting, storing, and using Plaintiff's and the Class members' biometric identifiers and biometric information as described herein, Ring violated the rights of Plaintiff and

each Class member to keep private these biometric identifiers and biometric information, as set forth in BIPA.

46. Individually and on behalf of the proposed Class, Plaintiff seeks: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Ring to comply with the BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein; (2) statutory damages for each intentional and reckless violation of the BIPA pursuant to 740 ILCS 14/20 (2), or alternatively, statutory damages pursuant to 740 ILCS 14/20(1) if the Court finds that Ring's violations were negligent; and (3) reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff as representative of the Class and appointing her counsel as Class Counsel;

B. Declaring that Ring's actions, as set out above, violate the BIPA, 740 ILCS 14/1, *et seq.*;

C. Awarding statutory damages for each and every intentional and reckless violation of the BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages pursuant to 740 ILCS 14/20(1) if the Court finds that Ring's violations were negligent;

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, *inter alia*, an Order requiring Ring to collect, store, and use biometric identifiers or biometric information in compliance with the BIPA;

E. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

F. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and

G. Awarding such other and further relief as equity and justice may require.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury for all issues so triable.

Dated: March 26, 2020

Respectfully submitted,

/s/ Kyle A. Shamberg

Kyle A. Shamberg
Nicholas R. Lange
CARLSON LYNCH, LLP
111 W. Wacker Drive, Suite 1240
Chicago, IL 60602
Telephone: 312-750-1265
kshamberg@carlsonlynch.com
nlange@carlsonlynch.com
Cook County ID No.: 63746

Liaison Counsel for Plaintiff and the Putative Class

Natalie F. Finkelman
Jayne A. Goldstein (IL Bar No. 6310724)
James C. Shah
SHEPHERD, FINKELMAN, MILLER & SHAH, LLP
1845 Walnut Street, Suite 806
Philadelphia, PA 19103
Telephone: 877-891-9880
nfinkelman@sfmslaw.com
jgoldstein@sfmslaw.com
jshah@sfmslaw.com

Counsel for Plaintiff and the Putative Class